Μαρούσι, 13 Ιουνίου 2017
Αρ. πρωτ.: 1794
ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ

(αριθμ: 194/2017)

Θέμα: Κλήση σε ακρόαση της εταιρείας με την επωνυμία «……...» με αντικείμενο τον έλεγχο της ενδεχόμενης παραβάσεως της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β΄2715/17-11-2011), σχετικά με τις αποκλίσεις από την εγκεκριμένη με την υπ' αριθμ. 50/2015 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 8 Νοεμβρίου 2016 Έκθεση Διενέργειας τακτικού Ελέγχου στην εν λόγω εταιρεία.

Την Τετάρτη, 7η Ιουνίου 2017, η Ολομέλεια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, παρισταμένων του Προέδρου της Αρχής κ. Χρήστου Ζαμπίρα, του Αντιπροέδρου κ. Μιχαήλ Σακκά, καθώς και των τακτικών μελών κ.κ. Μιχαήλ Γεωργιακόδη, Γεωργίου Μπακάλη και Αικατερίνης Παπανικολάου και απόντων των τακτικών μελών κ.κ. Ιωάννη Ασκοξυλάκη και Παναγιώτη Ριζομυλιώτη, οι οποίοι δεν παρέστησαν λόγω κωλύματος, αν και είχαν νομίμως και εμπροθέσμως προσκληθεί, και παρόντος του αναπληρωματικού μέλους κου Δημοσθένη Βουγιούκα, ο οποίος προσήλθε προς αναπλήρωση του τακτικού μέλους κ. Ασκοξυλάκη, συνήλθε σε συνεδρίαση προκειμένου να αποφασίσει επί της ενδεχόμενης κλήσης σε ακρόαση της εταιρείας με την επωνυμία «…….», με αντικείμενο τον έλεγχο της ενδεχόμενης παραβάσεως της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β΄2715/17-11-2011) (εφεξής «Κανονισμός»), σχετικά με τις αποκλίσεις από την εγκεκριμένη με την υπ' αριθμ. 50/2015 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 8 Νοεμβρίου 2016 Έκθεση Διενέργειας τακτικού Ελέγχου στην εν λόγω εταιρεία, αναφορικά με την εφαρμογή της Πολιτικής διασφάλισης του απορρήτου των επικοινωνιών. Τα μέλη της Ολομέλειας δήλωσαν ότι ενημερώθηκαν για τη μέχρι σήμερα εξέλιξη της υπόθεσης και ότι έλαβαν πλήρη γνώση αυτής.

Α. Σύμφωνα με την από 8 Νοεμβρίου 2016 Έκθεση Διενέργειας τακτικού Ελέγχου αναφορικά με την εφαρμογή της Πολιτικής διασφάλισης του απορρήτου των επικοινωνιών στην εταιρεία «……...» παρατηρήθηκαν αποκλίσεις από την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της ως άνω εταιρείας, όπως αυτή εγκρίθηκε με την υπ' αριθμ. 50/2015 Απόφαση της Α.Δ.Α.Ε.. Τα αποτελέσματα του τακτικού ελέγχου έχουν ως εξής :

«Γ. ΕΞΕΤΑΣΗ ΣΤΟΙΧΕΙΩΝ – ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΟΥ ΕΛΕΓΧΟΥ

Η Ο.Ε. κατά τους επιτόπιους ελέγχους, αλλά και από την εξέταση των στοιχείων που παρέλαβε, έλεγξε δειγματοληπτικά την εφαρμογή της εγκριθείσας Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των επικοινωνιών. Ειδικότερα, έλεγξε συγκεκριμένα σημεία των επιμέρους πολιτικών και διαδικασιών όπως αναλύεται παρακάτω:

1. **Συμμόρφωση με τις παρατηρήσεις που περιλαμβάνονται στην από 17.4.2015 Έκθεση Ελέγχου Συμμόρφωσης Πολιτικής της εταιρείας, η οποία επισυνάπτεται στην υπ' αριθμ. 50/2015 Απόφαση της ΑΔΑΕ (αρ. πρωτ. ΑΔΑΕ 1180/17.6.2015)**

Η εταιρεία, με το υπ.αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ17/4.2.2016 έγγραφό της (Σχετικό 7), έστειλε στην ΑΔΑΕ διευκρινίσεις σχετικά με τη συμμόρφωση με τις παρατηρήσεις που περιλαμβάνονται στην από 17.4.2015 Έκθεση Ελέγχου Συμμόρφωσης της με αρ. πρωτ. ΑΔΑΕ ΕΜΠ22/10.03.2015 Πολιτικής Ασφάλειας της εταιρείας ……., η οποία επισυνάπτεται στην Απόφαση 50/2015 της ΑΔΑΕ, χωρίς όμως να έχει συμπληρώσει αντίστοιχα το κείμενο της Πολιτικής Ασφάλειας που διαθέτει.

Παρατήρηση 1: Η εταιρεία οφείλει να συμπληρώσει την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της, σύμφωνα με τις παρατηρήσεις που διατυπώνονται στην από 17.4.2015 Έκθεση Ελέγχου Συμμόρφωσης.

2. **Υλοποίηση της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών (Άρθρο 3 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Παράγραφος 3.2.3 - Αδυναμίες Συμμόρφωσης (Πολιτική Ασφάλειας/Γενικές Αρχές, σελίδα 3, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία δήλωσε στο Σχετικό 5 ότι δεν υπάρχουν αδυναμίες συμμόρφωσης.

Περαιτέρω, από την εξέταση του Συνημμένου 1 του Σχετικού 5, προκύπτει ότι η εταιρεία αναφέρει ότι η διαδικασία καταγραφής και τεκμηρίωσης των αδυναμιών της παραγράφου 3.2.3 αντιστοιχεί στη διαδικασία με σήμανση 6.8.8/σ.79. Πλην όμως, η διαδικασία 6.8.8 έχει τίτλο «Διαδικασία Διαχείρισης Ευπαθειών» και έχει περιεχόμενο που δε σχετίζεται με την καταγραφή αδυναμιών συμμόρφωσης.

Παρατήρηση 2: Η εταιρεία οφείλει να συντάξει τη διαδικασία καταγραφής και τεκμηρίωσης των αδυναμιών συμμόρφωσης με τις απαιτήσεις που ορίζονται στην Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

Παράγραφος 3.2.4 - Διαδικασίες (Πολιτική Ασφάλειας/Γενικές Αρχές, σελίδες 3-4, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε με το Συνημμένο 1 του Σχετικού 5 τις διαδικασίες που ορίζονται στην πολιτική ασφάλειας της εταιρείας, όπως ζητήθηκαν με το Σχετικό 4. Σύμφωνα με τον Κατάλογο Διαδικασιών, που επισυνάπτει η εταιρεία στο Συνημμένο 1 του Σχετικού 5, προκύπτει αντιστοίχιση των διαδικασιών με επιμέρους παραγράφους ενός κειμένου με σήμανση Π2.1, το οποίο φαίνεται να έχει τίτλο «Εγχειρίδιο Συστήματος Διαχείρισης Ασφάλειας, Έκδοση 1». Πλην όμως, το κείμενο αυτό δεν έχει παραδοθεί στο σύνολό του και δεν έχει τη σχετική αρίθμηση σελίδων του Καταλόγου Διαδικασιών.

Παρατήρηση 3: Η εταιρεία οφείλει να διατηρεί τις διαδικασίες της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών με επιμέλεια και ευκρίνεια.

Παράγραφος 3.2.9 – Ειδικό Σχέδιο Αρχείων Καταγραφής (Πολιτική Ασφάλειας/Γενικές Αρχές, σελίδα 4, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία, στο Σχετικό 5, δήλωσε ότι χρησιμοποιείται κεντρικό σύστημα αρχείων καταγραφής (log manager), και επιπλέον παρέδωσε, με το Συνημμένο 1 του Σχετικού 6, το Ειδικό Σχέδιο Αρχείων Καταγραφής. Το Σχέδιο αναφέρει ότι «*για την πρόσβαση στο σύστημα …….το οποίο επιτρέπει την αναζήτηση εγγραφών, απαιτείται κωδικός. Η πρόσβαση στο σύστημα αυτό είναι κρυπτογραφημένη μέσω HTTPS. Ο Log Server καταχωρεί όλες τις εγγραφές που λαμβάνει σε βάση δεδομένων ……..η οποία φιλοξενείται στο ίδιο μηχάνημα*». Επομένως, η απαίτηση σχετικά με την εμπιστευτικότητα των αρχείων καταγραφής επιτυγχάνεται μερικώς, δεδομένου ότι, παρόλο που δεν προβλέπεται κρυπτογράφηση των εγγραφών που καταχωρούνται στο σύστημα, η πρόσβαση σε αυτές είναι ελεγχόμενη και κρυπτογραφημένη.

Παρατήρηση 4: Η εταιρεία οφείλει να διερευνήσει τη δυνατότητα κρυπτογράφησης των εγγραφών στη βάση δεδομένων …….. του κεντρικού συστήματος αρχείων καταγραφής.

Παράγραφος 3.3.1.1 - Κατάλογος ΠΕΣ (Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου, σελίδα 6, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε τα Συνημμένα 2α, 2β και 2γ του Σχετικού 5, τα οποία περιλαμβάνουν τις Μονάδες Εξυπηρετητών Κέντρου Δεδομένων, τις Μονάδες Εξυπηρετητών Κύριας Τοποθεσίας και τις Μονάδες Εξυπηρετητών Σύννεφου αντίστοιχα. Τα έγγραφα περιλαμβάνουν διάφορες πληροφορίες για τα συστήματα, όπως το όνομα, η διεύθυνση IP, ο ρόλος, ο τύπος και το μοντέλο, το λειτουργικό σύστημα, τα δεδομένα που διατηρεί και η διαθεσιμότητα.

Παράγραφος 3.3 - Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου (Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου, σελίδες 6-7, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία, στο Σχετικό 5, δήλωσε ότι τα αποτελέσματα της Αποτίμησης Πληροφοριακού Κινδύνου περιλαμβάνονται στο Συνημμένο 1 του Σχετικού 5. Σε αυτό περιέχεται έγγραφο με τίτλο «Παραδοτέο Π1.1, Τεύχος Ανάλυσης Επικινδυνότητας (Risk Analysis)» με ημερομηνία Μάιος 2016. Το έγγραφο, ενδεικτικά, περιέχει πληροφορίες σχετικά με το πλαίσιο μελέτης ανάλυσης και διαχείρισης επικινδυνότητας, την αξιολόγηση αγαθών των πληροφοριακών συστημάτων, την εκτίμηση της επικινδυνότητας και τη διαχείριση της επικινδυνότητας. Το έγγραφο, στην ενότητα «Συμπεράσματα Ανάλυσης Επικινδυνότητας» καταλήγει σε τρία συμπεράσματα υψηλής επικινδυνότητας, από τα οποία το ένα σχετίζεται με τη διαθεσιμότητα των υπηρεσιών (έλλειψη μηχανισμού πυρόσβεσης) το οποίο δεν αφορά στην Απόφαση 165/2011.

Παρατήρηση 5: Η εταιρεία οφείλει να λάβει υπόψη τα συμπεράσματα της αποτίμησης επικινδυνότητας για την αναθεώρηση της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και την υλοποίηση των κατάλληλων μέτρων για την εφαρμογή της.

3. Υλοποίηση της Πολιτικής Αποδεκτής Χρήσης (Άρθρο 4 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 4.2.1 - Αποδοχή Πολιτικής Ασφάλειας (Πολιτική Αποδεκτής Χρήσης/Γενικές Αρχές, σελίδα 9, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε δείγματα του σχετικού ειδικού παραρτήματος στη σύμβαση εργασίας των υπαλλήλων και συνεργατών της (Συνημμένα 3α και 3β του Σχετικού 5) και επιπλέον επέδειξε κατά τη διάρκεια του πρώτου επιτόπιου ελέγχου (Σχετικό 5) τις σχετικές φόρμες για τρεις υπαλλήλους με τις υπογραφές αυτών.

Παράγραφος 4.3.1 - Αρχείο Συνεργατών (Πολιτική Αποδεκτής Χρήσης/Απαιτήσεις Αναφορικά με τους Συνεργάτες, σελίδα 9, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε έγγραφο με κατάλογο συνεργατών (Συνημμένο 4 του Σχετικού 5). Στο έγγραφο περιλαμβάνονται τα στοιχεία τεσσάρων συνεργατών με επωνυμίες: ……., ……., …….., και ……...

Παράγραφος 4.3.2 – Ελάχιστο Περιεχόμενο Συμβάσεων με Συνεργάτες (Πολιτική Αποδεκτής Χρήσης/Απαιτήσεις Αναφορικά με τους Συνεργάτες, σελίδα 10, της εγκριθείσας Πολιτικής της εταιρείας)

Η Ο.Ε. ζήτησε τις συμβάσεις με τους ως άνω συνεργάτες της εταιρείας, όπως περιλαμβάνονται στο Συνημμένο 4 του Σχετικού 5, και η εταιρεία παρέδωσε τις εν λόγω συμβάσεις με τα Συνημμένα 5α (……), 5β (……..) και 5γ (……) του Σχετικού 5, καθώς με το Συνημμένο 2 (…….) του Σχετικού 6.

Από την εξέταση των ως άνω συμβάσεων προκύπτει ότι, παρόλο που αυτές περιλαμβάνουν γενικούς όρους εμπιστευτικότητας, μη αποκάλυψης και τήρησης απορρήτου, δεν γίνεται ειδική αναφορά σε συγκεκριμένες απαιτήσεις και μέτρα ασφάλειας που λαμβάνονται για τη διασφάλιση του απορρήτου των

επικοινωνιών, με τα οποία να διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων επικοινωνίας κατά την επεξεργασία αυτών, καθώς και η οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.

Απόκλιση 1: Εφαρμόζεται μερικώς η ενότητα «Απαιτήσεις Αναφορικά με τους Συνεργάτες» της εγκριθείσας Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας (παράγραφος 4.3.2 της Απόφασης 165/2011), δεδομένου ότι οι συμβάσεις δεν περιλαμβάνουν απαιτήσεις και μέτρα ασφάλειας που λαμβάνονται για τη διασφάλιση του απορρήτου των επικοινωνιών, με τα οποία διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων επικοινωνίας κατά την επεξεργασία αυτών, καθώς και η οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.

4. **Υλοποίηση της Πολιτικής Φυσικής Ασφάλειας (Άρθρο 5 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Παράγραφος 5.2.3 – Εξουσιοδότηση Φυσικής Πρόσβασης (Πολιτική Φυσικής Ασφάλειας, σελίδα 12, της εγκριθείσας Πολιτικής της εταιρείας)

Σχετικά με το αρχείο με το ιστορικό όλων των φυσικών προσβάσεων που έχουν εγκριθεί, η εταιρεία δήλωσε ότι τα σχετικά στοιχεία διατηρούνται στο σύστημα καταγραφής φυσικής πρόσβασης (……..) και παρέδωσε το αρχείο αυτό για το διάστημα από 1.5.2016 έως 6.6.2016 (Συνημμένο 7α και 7β του Σχετικού 5). Επιπρόσθετα, ο εκπρόσωπος της εταιρείας δήλωσε ότι σχετική πληροφορία διατηρείται σε έγγραφο με τίτλο «Αρχείο Φυσικών Προσβάσεων» το οποίο παραδόθηκε στην Ο.Ε. (Συνημμένο 7γ του Σχετικού 5).

Παράγραφοι 5.2.4 & 5.2.5 - Πρόσβαση σε χώρους ΠΕΣ και Καταγραφή Πρόσβασης (Πολιτική Φυσικής Ασφάλειας, σελίδα 12, της εγκριθείσας Πολιτικής της εταιρείας)

Σύμφωνα με τα διαλαμβανόμενα στο Σχετικό 5, η πρόσβαση στο computer room της εταιρείας γίνεται αποκλειστικά με ειδικό καρταναγνώστη, ενώ γίνεται καταγραφή της πρόσβασης σε βάση δεδομένων Access. Το σύστημα πρόσβασης με καρταναγνώστη λειτούργησε από 22.4.2016, όπως δήλωσε η εταιρεία, σύμφωνα με το Σχετικό 5. Επίσης, διαπιστώθηκε ότι στο χώρο του computer room υπάρχει εγκατεστημένη κάμερα καταγραφής κίνησης.

Τα μέλη της Ο.Ε. ζήτησαν και παρέλαβαν το αρχείο καταγραφής πρόσβασης στο computer room για το διάστημα από 1.5.2016 έως 6.6.2016 (Συνημμένο 6 του Σχετικού 5). Από την εξέταση του εν λόγω αρχείου, προκύπτει ότι το αρχείο καταγραφής ξεκινά να έχει καταγραφές από 4.5.2016. Επίσης, στο αρχείο δεν περιλαμβάνεται σήμανση σχετικά με το αν το γεγονός που καταγράφεται αναφέρεται σε είσοδο ή έξοδο από το χώρο του computer room, παρά μόνο η περιγραφή (Description) με την ένδειξη «swipe». Περαιτέρω, από την αντιπαραβολή του εν λόγω αρχείου με το αρχείο με το ιστορικό όλων των φυσικών προσβάσεων που έχουν εγκριθεί (Συνημμένα 7α, 7β και 7γ του Σχετικού 5), προκύπτει αντιστοίχιση των υπαλλήλων για τους οποίους έχει δοθεί έγκριση πρόσβασης και αυτών που απέκτησαν πρόσβαση στο χώρο του computer room.

Απόκλιση 2: Η εταιρεία δεν είχε εγκαταστήσει σύστημα ελεγχόμενης πρόσβασης στους χώρους ΠΕΣ εντός της εταιρείας (computer room) έως την 22.4.2016 και δεν εφάρμοζε την καταγραφή πρόσβασης σε αυτούς τους χώρους έως την 4.5.2016. Επισημαίνεται ότι σύμφωνα με την Απόφαση της ΑΔΑΕ υπ.αριθμ. 50/2015 (Σχετικό 3) που παραδόθηκε στην εταιρεία την 16.7.2015 (αρ. πρωτ. ΑΔΑΕ 1446/16.7.2015, Σχετικό 8), η εταιρεία είχε υποχρέωση να έχει υλοποιήσει και να εφαρμόζει την εγκριθείσα πολιτική ασφάλειας την 16.1.2016 (6 μήνες από την παραλαβή).

Παρατήρηση 6: Η εταιρεία οφείλει να εξασφαλίσει ότι η καταγραφή των προσβάσεων στους χώρους ΠΕΣ καταγράφει τόσο την ώρα εισόδου όσο και την ώρα εξόδου, σύμφωνα με τις παραγράφους 5.2.4 και 5.2.5 της Απόφασης 165/2011.

5. **Υλοποίηση της Πολιτικής Λογικής Πρόσβασης (Άρθρο 6 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Παράγραφος 6.2.1 – Αρχείο Μηχανισμών Ελέγχου Πρόσβασης και Αυθεντικοποίησης (Πολιτική Λογικής Πρόσβασης, Γενικές Αρχές, σελίδα 13, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε σχετικά το Συνημμένο 4 του Σχετικού 6, το οποίο περιλαμβάνει την τοπολογία των συστημάτων αυθεντικοποίησης, τους τρόπους πρόσβασης χρηστών του …… σε συστήματα που είναι κάτω από το …… των ……, την αυθεντικοποίηση υπαλλήλων στους σταθμούς εργασίας και σε συστήματα της εταιρείας, την αυθεντικοποίηση σε εσωτερικές εφαρμογές της ……, τους τρόπους αυθεντικοποίησης επιμέρους συστημάτων και τη συχνότητα αλλαγής συνθηματικών.

Παράγραφος 6.2.2 – Αντιστοίχιση Λογαριασμών Πρόσβασης (Πολιτική Λογικής Πρόσβασης, Γενικές Αρχές, σελίδα 13, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε σχετικά εκτύπωση του αρχείου αντιστοίχισης λογαριασμών-εργαζομένων, το οποίο αποτυπώνει την τρέχουσα κατάσταση (Συνημμένο 6α του Σχετικού 6, πριν την εφαρμογή του ……) και (Συνημμένο 6β του Σχετικού 6, μετά την εφαρμογή του ……..).

Επισημαίνεται ότι μόνο στο Συνημμένο 6β του Σχετικού 6 αναγράφεται στο αρχείο το όνομα χρήστη (username) του εκάστοτε εργαζομένου.

Παράγραφος 6.2.6 - Πρόσβαση σε Δεδομένα Επικοινωνίας (Πολιτική Λογικής Πρόσβασης, σελίδες 13-14, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε, με το Συνημμένο 8 του Σχετικού 5, πίνακα που περιλαμβάνει 38 είδη δεδομένων (δεν αφορούν όλα σε δεδομένα επικοινωνίας) και για κάθε ένα από αυτά, τη διαβάθμιση, τον ιδιοκτήτη πληροφοριών, τη δυνατότητα πρόσβασης ανά εργαζόμενο της εταιρείας και το σύστημα μέσω του οποίου αποκτάται η πρόσβαση.

Παράγραφος 6.2.5 - Αρχεία Καταγραφής Πρόσβασης (Πολιτική Λογικής Πρόσβασης, σελίδα 13, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρείχε διευκρινίσεις σχετικά με τη λογική πρόσβαση στα συστήματα …… και …….. (από τον πίνακα του Συνημμένου 2β του Σχετικού 5) σε επίπεδο λειτουργικού συστήματος και σχετικά με την εφαρμογή διαχείρισης τηλεφωνίας (…….) αυτών.

Πιο συγκεκριμένα, σχετικά με τον τρόπο υλοποίησης της λογικής πρόσβασης στα συστήματα …… και ……. σε επίπεδο λειτουργικού συστήματος, η εταιρεία ανέλυσε την αρχιτεκτονική που έχει υλοποιηθεί με χρήση …… και …… (……). Με αυτή την διάταξη επιτυγχάνεται κεντρική διαχείριση λογαριασμών και single sign on. Στα εν λόγω συστήματα πρόσβαση έχει μόνο ο χρήστης …… που ανήκει στο group superman (Συνημμένα 9α και 9β του Σχετικού 5) και η εταιρεία …….. με δικαιώματα ……, για την οποία η πρόσβαση επιτρέπεται μόνο από συγκεκριμένες IP διευθύνσεις.

Η εταιρεία, περαιτέρω, παρέδωσε, με το Συνημμένο 13 του Σχετικού 5 (οπτικός δίσκος), τις προσβάσεις των χρηστών στα συστήματα …… και ……. Από την εξέταση των αρχείων καταγραφής που περιέχονται στον οπτικό δίσκο προκύπτει ότι τα αρχεία καταγραφής καλύπτουν το χρονικό διάστημα από 8.5.2016 έως 6.6.2016 και όχι από 1.3.2016 όπως ζητήθηκε από την Ο.Ε. με το Σχετικό 5. Περαιτέρω, επισημαίνεται ότι το εν λόγω αρχείο περιλαμβάνει την ώρα πρόσβασης στο σύστημα (session opened for user…), καθώς και την ώρα αποσύνδεσης από το σύστημα (session closed for user…) για κάθε χρήστη που αποκτά πρόσβαση, καταγράφοντας το όνομα χρήστη (username) και την διεύθυνση IP από την οποία αυτός συνδέθηκε. Τέλος, το αρχείο καταγραφής περιλαμβάνει και τις ανεπιτυχείς προσπάθειες απόκτησης πρόσβασης (Failed password for…) καταγράφοντας παράλληλα και την διεύθυνση IP από την οποία ο χρήστης προσπάθησε να συνδεθεί.

Απόκλιση 3: Η εταιρεία δεν προσκόμισε τις προσβάσεις των χρηστών στα συστήματα ……. και ……. σε επίπεδο λειτουργικού συστήματος για το χρονικό διάστημα από 1.3.2016 έως 6.6.2016, όπως ζητήθηκε κατά τον πρώτο επιτόπιο έλεγχο (Σχετικό 5), αλλά από 8.5.2016 έως 6.6.2016.

Σχετικά με την πρόσβαση στην εφαρμογή διαχείρισης τηλεφωνίας (…….), η εταιρεία επέδειξε τα groups που έχουν δικαίωμα πρόσβασης στην πλατφόρμα και αναφέρθηκε ειδικά στο group accountant στο οποίο ανήκουν οι διαχειριστές της εφαρμογής. Τα μέλη της Ο.Ε. ζήτησαν και παρέλαβαν λίστα με τους λογαριασμούς αυτού του group (Συνημμένο 10 του Σχετικού 5).

Τα μέλη της Ο.Ε. ζήτησαν τις προσβάσεις των χρηστών του Συνημμένου 10 στην εφαρμογή διαχείρισης τηλεφωνίας από 5.5.2016 έως 5.6.2016 και ο εκπρόσωπος της εταιρείας παρέδωσε τα Συνημμένα 12α, 12β και 12γ του Σχετικού 5.

Από την εξέταση των ως άνω συνημμένων αρχείων προκύπτει ότι αυτά αποτελούν εκτυπώσεις φύλλων του excel (……..) και αφορούν στους υπαλλήλους …… (Συνημμένο 12α του Σχετικού 5), ……. (Συνημμένο 12β του Σχετικού 5) και ……. (Συνημμένο 12γ του Σχετικού 5). Τα ονόματα αυτά περιλαμβάνονται στους χρήστες του group accountant του Συνημμένου 10 του Σχετικού

5. Στα αρχεία αυτά περιλαμβάνεται η ημερομηνία και ώρα κατά την οποία ο χρήστης απέκτησε πρόσβαση (login) στο σύστημα, ενώ δεν εμφανίζεται η ώρα που τερματίστηκε η πρόσβαση.

Παρατήρηση 7: Η εταιρεία οφείλει να διατηρεί στα αρχεία καταγραφής πρόσβασης την ημερομηνία και ώρα τερματισμού της πρόσβασης στην εφαρμογή διαχείρισης τηλεφωνίας (……).

Παράγραφος 6.3.1 - Διαδικασία Διαχείρισης Χρηστών ΠΕΣ (σελίδα 14 της εγκριθείσας Πολιτικής της εταιρείας)

Στη συνέχεια, τα μέλη της Ο.Ε. ζήτησαν τις αιτήσεις πρόσβασης των χρηστών του Συνημμένου 10 του Σχετικού 5 σύμφωνα με τη διαδικασία διαχείρισης χρηστών και ο εκπρόσωπος της εταιρείας δήλωσε, στο Σχετικό 5, ότι δεν υπάρχουν οι σχετικές αιτήσεις. Πλην όμως, δήλωσε ότι η σχετική πληροφορία διατηρείται σε έγγραφο με τίτλο «Λογαριασμοί Πρόσβασης», το οποίο παρέδωσε στα μέλη της Ο.Ε. (Συνημμένο 11 του Σχετικού 5).

Από την εξέταση του ως άνω αρχείου προκύπτει ότι, για τον χρήστη «……», δεν υπάρχει καμία σχετική εγγραφή. Για τον χρήστη «……..» περιλαμβάνεται μία εγγραφή σχετικά με το ΠΕΣ «……». Τέλος, για τον χρήστη «……..», που συσχετίζεται με τον χρήστη «……..», σύμφωνα με το Συνημμένο 6β του Σχετικού 6, υπάρχουν τρεις εγγραφές για τα ΠΕΣ «….», «……» και «……..». Επισημαίνεται περαιτέρω ότι η ονοματολογία των ΠΕΣ στο εν λόγω έγγραφο δεν βρίσκεται σε αντιστοιχία με τον Κατάλογο ΠΕΣ (Συνημμένα 2α, 2β και 2γ του Σχετικού 5) που παρέδωσε η εταιρεία.

Περαιτέρω, κατά τον 2^{ο} επιτόπιο έλεγχο στις 21.6.2016, σχετικά με τις αιτήσεις πρόσβασης των χρηστών, σύμφωνα με τη διαδικασία διαχείρισης χρηστών, η εταιρεία δήλωσε ότι τώρα πλέον έχει υλοποιήσει τη διαδικασία για τη χορήγηση πρόσβασης σε νέους χρήστες και παρέδωσε τις αιτήσεις χορήγησης πρόσβασης σε πληροφοριακούς πόρους για όλους τους χρήστες (Συνημμένο 5α του Σχετικού 6, πριν την εφαρμογή του ……) και (Συνημμένο 5β του Σχετικού 6, μετά την εφαρμογή του ……).

Από την εξέταση του Συνημμένου 5α του Σχετικού 6 (πριν την εφαρμογή του ……), προκύπτει ότι υπάρχουν οι σχετικές αιτήσεις για τους χρήστες: ……., …… και ……, με ημερομηνία 1.12.2015. Από την εξέταση του Συνημμένου 5β του Σχετικού 6 (μετά την εφαρμογή του …….) επίσης προκύπτουν οι αιτήσεις για τους ως άνω χρήστες, με ημερομηνία 27.5.2016.

Απόκλιση 4: Η εταιρεία, κατά το χρόνο του πρώτου επιτόπιου ελέγχου, δεν εφάρμοζε την Διαδικασία Διαχείρισης Χρηστών ΠΕΣ, ως προς τη διατήρηση αρχείου των αιτήσεων που αφορούν σε κάθε μεταβολή στην κατάσταση πρόσβασης των χρηστών ΠΕΣ. Πλην όμως, η εταιρεία κατά το δεύτερο επιτόπιο έλεγχο δήλωσε πως έχει πλέον υλοποιήσει τη σχετική υποχρέωση και παρέδωσε σχετική τεκμηρίωση.

Παρατήρηση 8: Η εταιρεία οφείλει να χρησιμοποιεί την ίδια ονοματολογία για τα ΠΕΣ σε όλα τα αρχεία τεκμηρίωσης της Πολιτικής της.

Παρατήρηση 9: Η εταιρεία οφείλει να διατηρεί αρχείο με τεκμηρίωση όλων των συστημικών λογαριασμών πρόσβασης (system accounts) που έχουν οριστεί στα ΠΕΣ της, με περιγραφή του ρόλου και της χρησιμότητάς τους.

Παράγραφος 6.4.1 & 6.4.2 – Κανόνες δημιουργίας και αλλαγής κωδικών πρόσβασης (σελίδα 14 της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε αρχείο με τίτλο «Περιγραφή κανόνων δημιουργίας ονόματος χρήστη, συνθηματικών, generic accounts» (Συνημμένο 7 του Σχετικού 6). Το εν λόγω έγγραφο περιέχει κανόνες για τη δημιουργία ονομάτων χρήστη (username), την πολιτική ισχυρών συνθηματικών, όπου, μεταξύ άλλων, αναφέρεται και η συχνότητα υποχρεωτικής αλλαγής τους (κάθε 90 ημέρες), οδηγίες για την κατασκευή συνθηματικών, και τα πρότυπα προστασίας συνθηματικών και συνθηματικών φράσεων.

Επιπρόσθετα, η εταιρεία δήλωσε, στο Σχετικό 6, ότι οι κανόνες και οι περιορισμοί των συνθηματικών στο …….. απεικονίζονται στο Συνημμένο 4 του Σχετικού 6 «Αρχείο Μηχανισμών Ελέγχου Πρόσβασης και Αυθεντικοποίησης σε κάθε ΠΕΣ». Τα μέλη της Ο.Ε., κατά τον 2^{ο} επιτόπιο έλεγχο (Σχετικό 6), διαπίστωσαν ότι οι ως άνω κανόνες και περιορισμοί έχουν εν τοις πράγμασι οριστεί στο ……..

6. Υλοποίηση της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης (Άρθρο 7 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 7.2.2 & 7.2.3 – Αρχεία Απομακρυσμένης Λογικής Πρόσβασης (Απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών, σελ. 17, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία διατηρεί αρχείο με τίτλο «Μονάδες Απομακρυσμένης Πρόσβασης», (Συνημμένο 8 του Σχετικού 6), στο οποίο καταγράφονται τα ΠΕΣ στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση, καθώς και οι εργαζόμενοι και συνεργάτες οι οποίοι έχουν εξουσιοδοτηθεί για χρήση της απομακρυσμένης πρόσβασης ανά ΠΕΣ. Το αρχείο, επιπλέον, περιλαμβάνει για κάθε ΠΕΣ, τον τεχνικό τρόπο απομακρυσμένης πρόσβασης (ενδεικτικά: ……., ……., ……..).

Παράγραφος 7.2.6 & 7.2.7 – Απομακρυσμένη Πρόσβαση συνεργατών για συγκεκριμένο χρονικό διάστημα (Απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών, σελ. 18, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία δήλωσε, στο Σχετικό 6, ότι, κατά το χρόνο διεξαγωγής του ελέγχου, δεν έχει υλοποιηθεί σχετικός μηχανισμός. Ωστόσο, είναι στα άμεσα πλάνα της εταιρείας να υλοποιήσει αυτόν τον μηχανισμό, ο οποίος θα βασίζεται σε IP tables. Σχετικά με το αρχείο που περιέχει τα αιτήματα πρόσβασης συνεργατών και τις σχετικές εγκρίσεις, η εταιρεία, στο Σχετικό 6, δήλωσε ότι όλη η σχετική πληροφορία διατηρείται σε μηνύματα ηλεκτρονικού ταχυδρομείου και ειδικά για την εταιρεία ……. στο σύστημα ticketing αυτής. Πλην όμως, δεδομένου ότι δεν έχει υλοποιηθεί ο ως άνω

μηχανισμός, δεν μπορεί να γίνει ουσιαστικός έλεγχος της απομακρυσμένης πρόσβασης συνεργατών για συγκεκριμένο χρονικό διάστημα μέσω της αντιπαραβολής με τα εγκεκριμένα αιτήματα πρόσβασης των συνεργατών.

Απόκλιση 5: Η εταιρεία δεν εφαρμόζει τον περιορισμό της απομακρυσμένης πρόσβασης των συνεργατών της στα ΠΕΣ για συγκεκριμένο χρονικό διάστημα.

7. **Υλοποίηση της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ (Άρθρο 8 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Παράγραφος 8.2.3 - Αρχείο Αλλαγών ΠΕΣ (Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ, Γενικές Αρχές, σελίδα 19, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρέδωσε έντεκα (11) αιτήσεις αλλαγής υλικού ή λογισμικού με το Συνημμένο 9 του Σχετικού 6. Από την εξέταση των ως άνω αιτήσεων προκύπτει ότι το έγγραφο περιλαμβάνει τρία στάδια: το στάδιο προέγκρισης της αλλαγής (περιγραφή και αιτιολόγηση αυτής), το στάδιο με το σχέδιο υλοποίησης και δοκιμών (που περιλαμβάνει την αποτίμηση κινδύνου) και το στάδιο τελικής αποδοχής υλοποίησης και δοκιμών. Σε κάθε στάδιο προβλέπεται η αποδοχή (μέσω υπογραφής) από τους εκάστοτε υπεύθυνους, συμπεριλαμβανομένου του υπεύθυνου ασφάλειας. Οι έντεκα αλλαγές που παραδόθηκαν χρονολογούνται από 5.11.2015 έως 14.6.2016.

8. **Υλοποίηση της Πολιτικής Διαχείρισης Περιστατικών Ασφάλειας (Άρθρο 9 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Αναφορικά με τη διαδικασία διαχείρισης περιστατικών ασφάλειας, η εταιρεία δήλωσε, στο Σχετικό 6, ότι δεν έχουν αντιμετωπίσει κάποιο περιστατικό ασφάλειας και παρέδωσε υπόδειγμα Αναφοράς Περιστατικού Ασφάλειας (Συνημμένο 10 του Σχετικού 6).

9. **Υλοποίηση της Πολιτικής Ασφάλειας Δικτύου (Άρθρο 10 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Παράγραφοι 10.2.1 και 10.3.1 - Αρχιτεκτονική Ασφάλειας Δικτύου (Πολιτική Ασφάλειας Δικτύου, Γενικές Αρχές, σελίδα 23 και Λογικός Διαχωρισμός και Κατάτμηση Δικτύου, σελίδα 24, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία αρχικά παρέδωσε το Συνημμένο 14 του Σχετικού 5, το οποίο περιέχει σχηματική απεικόνιση του δικτύου της εταιρείας, καθώς και λίστα με τα …… και τους κανόνες του τοίχου προστασίας (firewall rules). Στη συνέχεια, κατά τον 2^{ο} επιτόπιο έλεγχο, η εταιρεία προσκόμισε το Αρχείο Κατάτμησης Δικτύου (Συνημμένο 3 του Σχετικού 6) που περιέχει την περιγραφή του δικτύου της εταιρείας, στα κεντρικά γραφεία της και στο ……., τα μέτρα προστασίας του εσωτερικού δικτύου της, τις υπηρεσίες

που παρέχονται σε συνδυασμό με σχηματική απεικόνιση των σχετικών κόμβων, περιγραφή των ζωνών ανά υπηρεσία και τις συνδέσεις με εξωτερικά δίκτυα.

10. **Υλοποίηση της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών (Άρθρο 11 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Παράγραφος 11.4 - Διεξαγωγή Ελέγχου (Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, Διεξαγωγή Ελέγχου, σελίδες 26-27 της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία, στο Σχετικό 6, δήλωσε ότι δεν έχει ακόμα διενεργηθεί ο εν λόγω έλεγχος, αλλά έχει προγραμματιστεί για το προσεχές μέλλον. Περαιτέρω, παρέδωσε έγγραφα με τίτλο «Στόχοι & Προγραμματισμός Εσωτερικής Επιθεώρησης Εφαρμογής» (Συνημμένο 11α του Σχετικού 6) και «Αναφορά Εσωτερικής Επιθεώρησης» (Συνημμένο 11β του Σχετικού 6), τα οποία θα χρησιμοποιηθούν ως υποδείγματα για τον εσωτερικό έλεγχο.

Επισημαίνεται ότι η εταιρεία οφείλει να πραγματοποιεί τον εν λόγω έλεγχο κατ' ελάχιστον ανά δύο (2) έτη, σύμφωνα με την παράγραφο 11.2.1 του Άρθρου 11 της Απόφασης 165/2011. Η εταιρεία είχε υποχρέωση να υλοποιήσει και να εφαρμόζει την εγκριθείσα πολιτική ασφάλειας την 16.1.2016, και συνεπώς, κατά το χρόνο διεξαγωγής του τακτικού ελέγχου, δεν είχε παρέλθει το διάστημα των δύο ετών.

11. **Υλοποίηση της Πολιτικής Αντιμετώπισης Κακόβουλου Λογισμικού (Άρθρο 12 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)**

Παράγραφος 12.2.3 – Έλεγχος Ακεραιότητας Λογισμικού των ΠΕΣ (Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού, Γενικές Αρχές, σελίδα 28, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία, στο Σχετικό 6, δήλωσε ότι δεν έχει πραγματοποιηθεί ο έλεγχος έως τώρα και ότι θα διαμορφωθούν οι κατάλληλοι μηχανισμοί στο προσεχές διάστημα.

Απόκλιση 6: Η εταιρεία δεν εφαρμόζει την απαίτηση της παραγράφου 12.2.3 της Απόφασης 165/2011, σχετικά με τον έλεγχο ακεραιότητας του λογισμικού των ΠΕΣ, με σκοπό τη διαπίστωση της μη ύπαρξης λογισμικού στα ΠΕΣ πέραν αυτού που έχει επισήμως προμηθευτεί η εταιρεία.

Παράγραφος 12.2.5 - Αρχείο Αντιμετώπισης Κακόβουλου Λογισμικού (Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού, Γενικές Αρχές, σελίδα 28, της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία, στο Σχετικό 6, δήλωσε ότι δε διατηρείται διακριτό αρχείο, αλλά σχετική πληροφορία περιέχεται στο Συνημμένο 3 του Σχετικού 6, στο οποίο γίνεται αναφορά στα συστήματα ……. Επιπρόσθετα, η εταιρεία παρέδωσε λίστα με τα αντίμετρα ασφάλειας των δύο

παραπάνω συστημάτων (Συνημμένα 12α και 12β του Σχετικού 6) και δήλωσε ότι το …….. προστατεύει τα συστήματα με λογισμικό ……..

Δ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από το δειγματοληπτικό έλεγχο εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας ……. κατά τους επιτόπιους ελέγχους και κατόπιν της εξέτασης των παρεληφθέντων στοιχείων διαπιστώθηκε ότι η εταιρεία ……, κατά το χρόνο διεξαγωγής του τακτικού ελέγχου, δεν εφήρμοζε πλήρως την εγκριθείσα, με την Απόφαση 50/2015 της ΑΔΑΕ, Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, ως προς τα σημεία που αναφέρονται αναλυτικά στην ενότητα Γ.»

Β. Η εν λόγω Έκθεση διενέργειας τακτικού ελέγχου στην εταιρεία «……..» εγκρίθηκε από την Ολομέλεια της Α.Δ.Α.Ε. σύμφωνα με το Πρακτικό της από 7 Δεκεμβρίου 2016 συνεδρίασης και η σχετική Απόφαση υπ' αριθμ. 364/2016 περί έγκρισης της διενέργειας του εν λόγω ελέγχου, μετά της συνημμένης έκθεσης, παρεδόθη στην εταιρεία «……...», όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 581/23-02-2017 Απόδειξη παράδοσης – παραλαβής.

Γ. Ενόψει των ανωτέρω και με βάση τα αποτελέσματα του διενεργηθέντος τακτικού ελέγχου στις εγκαταστάσεις της εταιρείας «…….», όπως αυτά αναλυτικά παρατίθενται ανωτέρω, αποδίδονται οι ακόλουθες ενδεχόμενες παραβάσεις της κείμενης νομοθεσίας σε σχέση με το απόρρητο των επικοινωνιών εκ μέρους της εταιρείας «……..»:

α) Ως προς την παρ. 4.3.2 της Πολιτικής Αποδεκτής Χρήσης

Από την εξέταση των συμβάσεων που έχει συνάψει η εταιρεία με συνεργάτες της, οι οποίοι έχουν πρόσβαση ή δύνανται να αποκτήσουν πρόσβαση σε δεδομένα επικοινωνίας συνδρομητών ή χρηστών των παρεχόμενων από αυτήν υπηρεσιών ή δικτύων προκύπτει ότι, παρόλο που αυτές περιλαμβάνουν γενικούς όρους εμπιστευτικότητας, μη αποκάλυψης και τήρησης απορρήτου, δεν γίνεται ειδική αναφορά σε συγκεκριμένες απαιτήσεις και μέτρα ασφάλειας που λαμβάνονται για τη διασφάλιση του απορρήτου των επικοινωνιών, με τα οποία να διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων επικοινωνίας κατά την επεξεργασία αυτών, καθώς και η οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.

Απόκλιση 1: Εφαρμόζεται μερικώς η ενότητα «Απαιτήσεις Αναφορικά με τους Συνεργάτες» της εγκριθείσας Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως προβλέπεται στην παράγραφο 4.3.2 της Απόφασης 165/2011 της Α.Δ.Α.Ε., δεδομένου ότι οι συμβάσεις δεν περιλαμβάνουν απαιτήσεις και μέτρα ασφάλειας που λαμβάνονται για τη διασφάλιση του απορρήτου των επικοινωνιών, με τα οποία διασφαλίζεται η εμπιστευτικότητα και ακεραιότητα των δεδομένων επικοινωνίας κατά την επεξεργασία αυτών, καθώς και η οριστική διαγραφή και καταστροφή αυτών μετά τη λήξη της συνεργασίας.

β) Ως προς τις παραγράφους 5.2.4 και 5.2.5 της Πολιτικής Φυσικής Ασφάλειας

Παράγραφοι 5.2.4 & 5.2.5 - Πρόσβαση σε χώρους ΠΕΣ και Καταγραφή Πρόσβασης (Πολιτική Φυσικής Ασφάλειας, σελίδα 12 της εγκριθείσας Πολιτικής της εταιρείας)

Σύμφωνα με τα ανωτέρω αποτελέσματα της έκθεσης ελέγχου, η πρόσβαση στο computer room της εταιρείας γίνεται αποκλειστικά με ειδικό καρταναγνώστη, ενώ γίνεται καταγραφή της πρόσβασης σε βάση δεδομένων Access. Το σύστημα πρόσβασης με καρταναγνώστη λειτούργησε από 22.4.2016, όπως δήλωσε η εταιρεία σχετικά. Επίσης, διαπιστώθηκε ότι στο χώρο του computer room υπάρχει εγκατεστημένη κάμερα καταγραφής κίνησης.

Τα μέλη της Ο.Ε. ζήτησαν και παρέλαβαν το αρχείο καταγραφής πρόσβασης στο computer room για το διάστημα από 1.5.2016 έως 6.6.2016. Από την εξέταση του εν λόγω αρχείου, προκύπτει ότι το αρχείο καταγραφής ξεκινά να έχει καταγραφές από 4.5.2016. Επίσης, στο αρχείο δεν περιλαμβάνεται σήμανση σχετικά με το αν το γεγονός που καταγράφεται αναφέρεται σε είσοδο ή έξοδο από το χώρο του computer room, παρά μόνο η περιγραφή (Description) με την ένδειξη «swipe». Περαιτέρω, από την αντιπαραβολή του εν λόγω αρχείου με το αρχείο με το ιστορικό όλων των φυσικών προσβάσεων που έχουν εγκριθεί, προκύπτει αντιστοίχιση των υπαλλήλων για τους οποίους έχει δοθεί έγκριση πρόσβασης και αυτών που απέκτησαν πρόσβαση στο χώρο του computer room.

Απόκλιση 2: Η εταιρεία δεν είχε εγκαταστήσει σύστημα ελεγχόμενης πρόσβασης στους χώρους ΠΕΣ εντός της εταιρείας (computer room) έως την 22.4.2016 και δεν εφάρμοζε την καταγραφή πρόσβασης σε αυτούς τους χώρους έως την 4.5.2016, όπως προβλέπεται στις παραγράφους 5.2.4 και 5.2.5 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε.. Επισημαίνεται ότι, σύμφωνα με την Απόφαση της ΑΔΑΕ υπ'αριθμ. 50/2015 περί έγκρισης της Πολιτικής Ασφάλειας της εταιρείας «……..», που παραδόθηκε στην εταιρεία την 16.7.2015 (αρ. πρωτ. ΑΔΑΕ 1446/16.7.2015), η εταιρεία είχε υποχρέωση να έχει υλοποιήσει και να εφαρμόζει την εγκριθείσα πολιτική

ασφάλειας την 16.1.2016, ήτοι μετά την παρέλευση 6 μηνών από την παραλαβή της απόφασης έγκρισης.

γ) Ως προς την παράγραφο 6.2.5 της Πολιτικής Λογικής Πρόσβασης

Παράγραφος 6.2.5 - Αρχεία Καταγραφής Πρόσβασης (Πολιτική Λογικής Πρόσβασης, σελίδα 13 της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία παρείχε διευκρινίσεις σχετικά με τη λογική πρόσβαση στα συστήματα …… και …….. σε επίπεδο λειτουργικού συστήματος και σχετικά με την εφαρμογή διαχείρισης τηλεφωνίας (…….) αυτών.

Πιο συγκεκριμένα, σχετικά με τον τρόπο υλοποίησης της λογικής πρόσβασης στα συστήματα …….. και ……. σε επίπεδο λειτουργικού συστήματος, η εταιρεία ανέλυσε την αρχιτεκτονική που έχει υλοποιηθεί με χρήση ……. και ……. (……..). Με αυτή τη διάταξη επιτυγχάνεται κεντρική διαχείριση λογαριασμών και single sign on. Στα εν λόγω συστήματα πρόσβαση έχει μόνο ο χρήστης …… που ανήκει στο group superman και η εταιρεία …… με δικαιώματα ……, για την οποία η πρόσβαση επιτρέπεται μόνο από συγκεκριμένες IP διευθύνσεις.

Η εταιρεία, περαιτέρω, παρέδωσε τις προσβάσεις των χρηστών στα συστήματα …. και ….. Από την εξέταση των αρχείων καταγραφής που περιέχονται στον οπτικό δίσκο προκύπτει ότι τα αρχεία καταγραφής καλύπτουν το χρονικό διάστημα από 8.5.2016 έως 6.6.2016 και όχι από 1.3.2016 όπως ζητήθηκε από την Ο.Ε. κατά τον πρώτο επιτόπιο έλεγχο στις εγκαταστάσεις της εταιρείας την 06-06-2016. Περαιτέρω, επισημαίνεται ότι το εν λόγω αρχείο περιλαμβάνει την ώρα πρόσβασης στο σύστημα (session opened for user…), καθώς και την ώρα αποσύνδεσης από το σύστημα (session closed for user…) για κάθε χρήστη που αποκτά πρόσβαση, καταγράφοντας το όνομα χρήστη (username) και την διεύθυνση IP από την οποία αυτός συνδέθηκε. Τέλος, το αρχείο καταγραφής περιλαμβάνει και τις ανεπιτυχείς προσπάθειες απόκτησης πρόσβασης (Failed password for…) καταγράφοντας παράλληλα και την διεύθυνση IP από την οποία ο χρήστης προσπάθησε να συνδεθεί.

Απόκλιση 3: Η εταιρεία δεν προσκόμισε τις προσβάσεις των χρηστών στα συστήματα ……. και …….. σε επίπεδο λειτουργικού συστήματος για το χρονικό διάστημα από 1.3.2016 έως 6.6.2016, όπως ζητήθηκε κατά τον πρώτο επιτόπιο έλεγχο της 06-06-2016, αλλά από 8.5.2016 έως 6.6.2016.

δ) Ως προς την παράγραφο 6.3.1 της Διαδικασίας Διαχείρισης Χρηστών ΠΕΣ της Πολιτικής Λογικής Πρόσβασης

Παράγραφος 6.3.1 - Διαδικασία Διαχείρισης Χρηστών ΠΕΣ (σελίδα 14 της εγκριθείσας Πολιτικής της εταιρείας)

Τα μέλη της Ο.Ε. ζήτησαν τις αιτήσεις πρόσβασης των χρηστών στην εφαρμογή διαχείρισης τηλεφωνίας (…….), σύμφωνα με τη διαδικασία διαχείρισης χρηστών και ο εκπρόσωπος της εταιρείας δήλωσε, όπως προκύπτει από το πρακτικό διενέργειας επιτόπιου ελέγχου της 06-06-2016, ότι δεν υπάρχουν οι σχετικές αιτήσεις. Πλην όμως, δήλωσε ότι η σχετική πληροφορία διατηρείται σε έγγραφο με τίτλο «Λογαριασμοί Πρόσβασης», το οποίο παρέδωσε στα μέλη της Ο.Ε..

Από την εξέταση του ως άνω αρχείου προκύπτει ότι, για τον χρήστη «…….», δεν υπάρχει καμία σχετική εγγραφή. Για τον χρήστη «…….» περιλαμβάνεται μία εγγραφή σχετικά με το ΠΕΣ «……». Τέλος, για τον χρήστη «……», που συσχετίζεται με τον χρήστη «……», υπάρχουν τρεις εγγραφές για τα ΠΕΣ «……», «……..» και «…….». Επισημαίνεται περαιτέρω ότι η ονοματολογία των ΠΕΣ στο εν λόγω έγγραφο δεν βρίσκεται σε αντιστοιχία με τον Κατάλογο ΠΕΣ που παρέδωσε η εταιρεία.

Περαιτέρω, κατά τον 2^{ο} επιτόπιο έλεγχο στις 21.6.2016, σχετικά με τις αιτήσεις πρόσβασης των χρηστών, σύμφωνα με τη διαδικασία διαχείρισης χρηστών, η εταιρεία δήλωσε ότι τώρα πλέον έχει υλοποιήσει τη διαδικασία για τη χορήγηση πρόσβασης σε νέους χρήστες και παρέδωσε τις αιτήσεις χορήγησης πρόσβασης σε πληροφοριακούς πόρους για όλους τους χρήστες.

Από την εξέταση των εν λόγω στοιχείων προκύπτει ότι υπάρχουν οι σχετικές αιτήσεις για τους ως άνω χρήστες, με ημερομηνία 1.12.2015, πριν την εφαρμογή του ……., καθώς και μετά την εφαρμογή του ……, με ημερομηνία 27.5.2016.

Απόκλιση 4: Η εταιρεία, κατά το χρόνο του πρώτου επιτόπιου ελέγχου, δεν εφάρμοζε την Διαδικασία Διαχείρισης Χρηστών ΠΕΣ, ως προς τη διατήρηση αρχείου των αιτήσεων που αφορούν σε κάθε μεταβολή στην κατάσταση πρόσβασης των χρηστών ΠΕΣ, όπως προβλέπεται στην παράγραφο 6.3.1 της Πολιτικής Λογικής Πρόσβασης. Πλην όμως, η εταιρεία κατά το δεύτερο επιτόπιο έλεγχο δήλωσε πως έχει πλέον υλοποιήσει τη σχετική υποχρέωση και παρέδωσε σχετική τεκμηρίωση.

ε) Ως προς τις παραγράφους 7.2.6 και 7.2.7 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης

Παράγραφος 7.2.6 & 7.2.7 – Απομακρυσμένη Πρόσβαση συνεργατών για συγκεκριμένο χρονικό διάστημα (Απομακρυσμένη πρόσβαση εργαζομένων και συνεργατών, σελ. 18 της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία δήλωσε, κατά το δεύτερο επιτόπιο έλεγχο της 21ης Ιουνίου 2016, ότι, κατά το χρόνο διεξαγωγής του ελέγχου, δεν έχει υλοποιηθεί σχετικός μηχανισμός. Ωστόσο, είναι στα άμεσα πλάνα της εταιρείας να υλοποιήσει αυτόν τον μηχανισμό, ο οποίος θα βασίζεται σε …….. Σχετικά με το αρχείο που περιέχει τα αιτήματα πρόσβασης συνεργατών και τις σχετικές εγκρίσεις, η εταιρεία δήλωσε ότι όλη η σχετική πληροφορία διατηρείται σε μηνύματα ηλεκτρονικού ταχυδρομείου και ειδικά για την εταιρεία ……. στο σύστημα ……. αυτής. Πλην όμως, δεδομένου ότι δεν έχει υλοποιηθεί ο ως άνω μηχανισμός, δεν μπορεί να γίνει ουσιαστικός έλεγχος της απομακρυσμένης πρόσβασης συνεργατών για συγκεκριμένο χρονικό διάστημα μέσω της αντιπαραβολής με τα εγκεκριμένα αιτήματα πρόσβασης των συνεργατών.

Απόκλιση 5: Η εταιρεία δεν εφαρμόζει τον περιορισμό της απομακρυσμένης πρόσβασης των συνεργατών της στα ΠΕΣ για συγκεκριμένο χρονικό διάστημα, όπως προβλέπεται στις παραγράφους 7.2.6 και 7.2.7 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε..

στ) Ως προς την παρ. 12.2.3 της Πολιτικής Αντιμετώπισης Κακόβουλου Λογισμικού

Παράγραφος 12.2.3 – Έλεγχος Ακεραιότητας Λογισμικού των ΠΕΣ (Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού, Γενικές Αρχές, σελίδα 28 της εγκριθείσας Πολιτικής της εταιρείας)

Η εταιρεία, κατά το δεύτερο επιτόπιο έλεγχο της 21ης Ιουνίου 2016, δήλωσε ότι δεν έχει πραγματοποιηθεί ο έλεγχος ακεραιότητας λογισμικού των ΠΕΣ έως τώρα και ότι θα διαμορφωθούν οι κατάλληλοι μηχανισμοί στο προσεχές διάστημα.

Απόκλιση 6: Η εταιρεία δεν εφαρμόζει την απαίτηση της παραγράφου 12.2.3 της Απόφασης 165/2011, σχετικά με τον έλεγχο ακεραιότητας του λογισμικού των ΠΕΣ, με σκοπό τη διαπίστωση της μη ύπαρξης λογισμικού στα ΠΕΣ πέραν αυτού που έχει επισήμως προμηθευτεί η εταιρεία.

Δ. Κατόπιν των παραπάνω, και έχοντας υπόψη:

1. Το άρθρο 19 του Συντάγματος,

2. Το ν.3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» (ΦΕΚ Α΄ 47/2003), όπως ισχύει,
3. Το ν. 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α' 136/10.07.2008), όπως ισχύει,
4. Τις διατάξεις του Κανονισμού για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (υπ' αριθμ. 165/2011 Απόφαση της Α.Δ.Α.Ε., ΦΕΚ Β΄2715/17.11.2011),
5. Το ν.3051/2002 «Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις» (ΦΕΚ Α' 220/2002), όπως ισχύει,
6. Το ν. 4055/2012 «Δίκαιη δίκη και εύλογη διάρκεια αυτής» (ΦΕΚ Α'51/2012), όπως ισχύει, και ιδίως τα άρθρα 61 και 110 παρ. 12 αυτού,
7. Την υπ' αριθμ. 97^{Α}/2012 Απόφαση της Α.Δ.Α.Ε. «Τροποποίηση της απόφασης της ΑΔΑΕ 44/31-10-2003 Απόφασης της ΑΔΑΕ "Κανονισμός Εσωτερικής Λειτουργίας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) (ΦΕΚ1642/Β/7.11.2003)", όπως ισχύει» (ΦΕΚ 1650/Β/11-05-2012 και 1751/Β/25-05-2012),
8. Τις διατάξεις της υπ' αριθμ. 44/31.10.2003 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός Εσωτερικής Λειτουργίας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)» (ΦΕΚ Β' 1642/7.11.2003), όπως ισχύει,
9. Το άρθρο 20 παρ. 2 του Συντάγματος, περί δικαιώματος προηγούμενης ακρόασης του διοικουμένου,
10. Τη διάταξη του άρθρου 26 παρ.7 του ν.4325/2015 «Εκδημοκρατισμός της Διοίκησης – Καταπολέμηση Γραφειοκρατίας και Ηλεκτρονική Διακυβέρνηση. Αποκατάσταση Αδικιών και άλλες διατάξεις» (ΦΕΚ Α' 47/2015),
11. Τη διάταξη του άρθρου 55 παρ.10 του ν.4339/2015 (ΦΕΚ Α' 133/2015) «Αδειοδότηση παρόχων περιεχομένου επίγειας ψηφιακής τηλεοπτικής ευρυεκπομπής ελεύθερης λήψης - Ίδρυση συνδεδεμένης με την Ε.Ρ.Τ. Α.Ε. ανώνυμης εταιρίας για την ανάπτυξη δικτύου επίγειας ψηφιακής ευρυεκπομπής - Ρύθμιση θεμάτων Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ. Τ.) - Εθνική Επικοινωνιακή Πολιτική, Οργάνωση της Επικοινωνιακής Διπλωματίας - Σύσταση Εθνικού Κέντρου Οπτικοακουστικών Μέσων και Επικοινωνίας και Μητρώου Επιχειρήσεων Ηλεκτρονικών Μέσων Ενημέρωσης - Τροποποίηση διατάξεων του Ν. 4070/2012 (Α' 82) και άλλες διατάξεις»,
12. Τη διάταξη του άρθρου 73 του ν. 4369/2016 (ΦΕΚ Α΄ 33/2016) «Εθνικό Μητρώο Επιτελικών Στελεχών Δημόσιας Διοίκησης, βαθμολογική διάρθρωση θέσεων, συστήματα

αξιολόγησης, προαγωγών και επιλογής προϊσταμένων (διαφάνεια – αξιοκρατία και αποτελεσματικότητα της Δημόσιας Διοίκησης) και άλλες διατάξεις»,

13. Την υπ' αριθμ. 16887/17-03-2016 Απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων (ΦΕΚ Υ.Ο.Δ.Δ. 151/21-03-2016), περί συγκρότησης της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών,
14. Τις διατάξεις του άρθρου εικοστού τρίτου του Ν. 4411/2016 (ΦΕΚ Α΄ 142/03-08-2016),
15. Την υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 22/10-03-2015 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας «……..», όπως αυτή εγκρίθηκε με την υπ' αριθμ. 50/2015 Απόφαση της Α.Δ.Α.Ε.,
16. Την υπ' αριθμ. 59/2016 Απόφαση της Α.Δ.Α.Ε. σχετικά με τη διενέργεια τακτικού ελέγχου στην εταιρεία «……..»,
17. Την υπ' αριθμ. 129/2016 Απόφαση του Προέδρου της Α.Δ.Α.Ε. σχετικά με τη σύσταση της Ομάδας Ελέγχου για τη διενέργεια τακτικού ελέγχου στην εταιρεία «……...»,
18. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις της εταιρείας «…….», με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 101/06-06-2016,
19. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις της εταιρείας «…….», με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 116/21-06-2016,
20. την από 08.11.2016 «Έκθεση Διενέργειας Τακτικού Ελέγχου στις εγκαταστάσεις της εταιρείας …….» με τα σχετικά αυτής,
21. Την υπ' αριθμ. 300/2016 Εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
22. Το πρακτικό της από 7 Δεκεμβρίου 2016 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,
23. Την υπ' αριθμ. 364/2016 Απόφαση της Α.Δ.Α.Ε. περί έγκρισης της ως άνω από 08-11-2016 Έκθεσης διενέργειας τακτικού ελέγχου στην εταιρεία «……», η οποία παραδόθηκε στην εταιρεία «…….», μετά της οικείας έκθεσης ελέγχου, συνημμένα στην υπ' αριθμ. πρωτ. ΑΔΑΕ 420/13-02-2017 επιστολή της Α.Δ.Α.Ε., όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 581/23-02-2017 Απόδειξη παράδοσης – παραλαβής,
24. Την υπ' αριθμ. 221/2017 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
25. Το πρακτικό της από 7 Ιουνίου 2017 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,
26. Την ανάγκη διασφάλισης του απορρήτου των επικοινωνιών,

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)
ΑΠΟΦΑΣΙΖΕΙ

την κλήση σε Ακρόαση της εταιρείας με την επωνυμία «……..», ενώπιον της Ολομέλειας της Α.Δ.Α.Ε., την **28η Ιουνίου 2017, ημέρα Τετάρτη και ώρα 13.30 μ.μ.**, στην έδρα της Α.Δ.Α.Ε., Ιερού Λόχου 3, Μαρούσι, με αντικείμενο τον έλεγχο της ενδεχόμενης παράβασης της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β΄2715/17-11-2011), σύμφωνα με τις αποκλίσεις που προσδιορίζονται στην εγκεκριμένη με την υπ' αριθμ. 50/2015 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 8 Νοεμβρίου 2016 Έκθεση Διενέργειας τακτικού Ελέγχου στην εν λόγω εταιρεία, αναφορικά με την εφαρμογή της Πολιτικής διασφάλισης του απορρήτου των επικοινωνιών και όπως αυτές αναλυτικά εκτίθενται ανωτέρω στο σημείο Γ της παρούσας.
Εισηγητής για την εν λόγω υπόθεση ορίζεται το τακτικό μέλος της Α.Δ.Α.Ε., κ. Παναγιώτης Ριζομυλιώτης.

Η παρούσα απόφαση να επιδοθεί στην εταιρεία «…….» με Δικαστικό Επιμελητή.
Κρίθηκε και αποφασίστηκε την 7 Ιουνίου 2017.

Ο Πρόεδρος

Χρήστος Ζαμπίρας